Stopping Rootkits at the Network Edge

January 2007

Trusted Computing Group 3855 SW 153rd Drive, Beaverton, OR 97006
TEL: (503) 619-0562 FAX: (503) 644-6708
admin@trustedcomputinggroup.org www.trustedcomputinggroup.org

Trusted Computing Group

Stopping Rootkits at the Network Edge

Keeping remote users' laptops healthy is not an easy task these days. Infections are everywhere, and once these PCs leave the shelter of an enterprise network, they can easily get filled with rootkits, trojan horses, spyware, and viruses.

Of the many types of infection, rootkits are the most troubling. A rootkit is a special software program that hides on a PC without the user's knowledge or permission. Rootkits can perform many nefarious functions, capturing and forwarding passwords and other confidential information, sending out spam, attacking other machines, or allowing remote control of the machine's operations. This can expose an enterprise to legal liability as well as potential data loss on the individual PCs that have been compromised.

The Trusted Computing Group (TCG) has been working for years to create building blocks for trusted hardware and software that makes PCs and other systems less vulnerable to rootkits and other malware. In this TCG white paper, we explore what makes rootkits so dangerous and how TCG technology can be used to stop their spread.

Why are rootkits dangerous?

First developed in the 1990s for Unix computers, rootkits became infamous for Windows PCs in 2005 when Sony Music used them in numerous music CDs to prevent users from making digital copies. Now they are quite common and basic prototypes are found on several Web sites that can be used by even inexperienced programmers to develop the most virulent rootkits.

What makes rootkits so insidious and distinctive is that they are hard to detect and harder still to remove without doing a wholesale operating system re-installation or re-imaging of a computer's hard drive. They are designed to hide from normal view of the operating system, since they modify the operating system itself. They can disguise themselves as ordinary operating system utilities, replacing the file and process viewing commands with their own code, or modify the most basic parts of the operating system (the kernel) to conceal their presence. Most of them are designed to survive reboots of the PC, and can live undetected on a system for months.

"Remember that a rootkit is not designed to help an intruder gain access to a system. A rootkit is designed to make the intruders feel at home and allow them to work silently on your system without being disturbed," says Oktay Altunergil, a web developer who has written about the topic.

Some of the nastier rootkits include key logging programs that will record username/passwords typed into a particular machine and send this information to a central repository that can be used to compromise or steal sensitive data.

A new breed of infections employs virtualization techniques similar to those used by EMC's VMware and Microsoft Virtual Server 2005. By silently creating a virtual environment in which the normal operating system runs, the rootkit gains access to all data processed by that operating system while evading detection.

How can rootkits be removed?

There are a series of rootkit detection and removal tools, such as Microsoft's own Malicious Software Removal, Sophos Anti-Rootkit, PrevX, Tripwire, UnHackMe and F-Secure's Blacklight. However, using any of these tools requires users to be vigilant and spend a lot of time pro-actively doing regular hard disk scans, along with spending time interpreting the results of these scans and deleting the offending compromised files. Even these countermeasures cannot always detect a kernel rootkit, which modifies the operating system kernel to hide itself. To detect a well-written kernel rootkit, users must boot a known clean copy of their OS from a special CD to bypass the rootkit and allow accurate detection. This is cumbersome at best.

However, most experts agree that having users reboot and scan PCs is not very practical on an ongoing basis, since most users are only going to investigate a potential rootkit issue once in a while. For example, users might be motivated to investigate a potential infection if some other symptom is observed on their PC, such as reduced performance or odd boot behavior. But well-written rootkits largely avoid such symptoms. Even PCs running their own firewall software are at risk, since infections can be transmitted by browsing dangerous Web pages or by sending files via Instant Messenger applications, or even by inserting a music CD into their systems, as Sony has so aptly demonstrated.

Trusted Platform Module (TPM)

The TPM is a special hardware component that is now present in most new commercial-grade laptops and desktops sold by the major PC manufacturers. According to IDC, a TPM is present in about 20 percent of all PCs operating today and ships with virtually every new enterprise model.

The TPM securely stores digital keys, certificates and passwords. Because it is security hardware, it is especially difficult to attack virtually or physically. It can protect keys using standard cryptographic algorithms and protocols that are widely accepted and will interoperate with other systems using software implementations. TPMs are sold complete with internal firmware so that the chip does not have to be programmed. The TPM can be used for a variety of purposes, including trusted software downloads, secure network communications, reliable identification of system peripherals, and secure local storage. See this white paper for further details: https://www.trustedcomputinggroup.org/groups/tpm/embedded_bkgdr_final_sept_14_2005.pdf

Copyright ©2004-2006 Trusted Computing Group (www.trustedcomputinggroup.org.) All Rights Reserved

What TCG is doing

But there is some good news on the rootkit prevention front. There are improvements in endpoint health assessment and remediation that can help to rid enterprises of rootkits by stopping them at their entry to a remote laptop. These measures take a combination of particular hardware and software and provide system administrators new ways to defend their PCs.

The developments center around a series of standards promoted by TCG that feature a piece of added hardware called the Trusted Platform Module (see sidebar).

Here is how the TPM works to stop rootkits and other infections: whenever the PC boots, the TPM measures the BIOS, boot loader, and all other critical software components in the operating system. These measurements are taken before the software runs and stored securely on the TPM so they can't be modified. When the PC connects to the network, the measurements are sent to a server where they are checked against a list of known good configurations. If the software is not good, the PC can be quarantined and repaired.

The TPM isn't the only thing that TCG is working on. In addition to the hardware, the consortium has also produced the Platform Trust Services (PTS), a set of software interfaces and architecture to measure the state of the machine and report on changes to its file system and memory (see sidebar). The Trusted Network Connect specifications complete the picture, providing a standard way to check and repair each endpoint whenever it connects to the network (see sidebar).

One company that has already developed software that works with the TPM is Wave Systems of Lee, Mass. They sell a product called Embassy Endpoint Enforcer, which is designed for use in enterprise IT endpoint situations to support the TPM hardware and ensure that no rootkits are operating on a remote laptop.

Wave's software forms the foundation of a new series of standards from the Trusted Computing Group called the Platform Trust Services, which became public in November 2006 (see sidebar for more information on PTS).

The specification for PTS defines how software can take advantage of the TPM and use it to determine how critical system components are measured and reported to the OS.

In addition to Wave, others are working on supporting the TPM, including Microsoft with its Vista operating system. Vista, which began shipping in December 2006 to corporate customers, includes a feature called BitLocker that provides hard drive encryption. The key for the encryption can be stored on the TPM chip, making it easy and secure.

The TPM with PTS and TNC gets around the issue of doing frequent system scans, because the boot process is guaranteed and no software can make any unauthorized modifications to these files. The TPM becomes the first step in the boot sequence, serving as a secure foundation for the BIOS, the boot loader, the kernel, and the rest of the operating system. Since the TPM performs this check every time the PC boots, it provides a regular check for rootkit infections. This means it will be easily apparent when a PC has been tampered with.

For more information, please contact:
Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97006
Email: admin@trustedcomputinggroup.org
Phone: (503) 619-0562, Fax: (503) 644-6708

Platform Trust Services (PTS)

TCG recently released a set of Platform Trust Services (PTS) specifications to provide a foundation for platform integrity measurement and verification. These include three key elements that together augment the ability to verify if any client system has been tampered or altered by rootkits and other malware, and can ensure that any system that uses a TPM can report its current state accurately and in a standard way. The three elements of PTS include:

- A set of *application programming interfaces* (APIs) for the measurement agent called the PTS Interface,
- A *common XML-based data format* for capturing and reporting integrity information in a client called the Integrity Schema,
- An overall *Integrity Management Architecture* that provides a common framework for collecting and reporting information about a trusted platform.

This set of specifications can be implemented with or without the presence of any TPM hardware although security is greater when a TPM is present. The PTS specification provides an agent that can be called to perform measurements of the components of the device, as well as other platform components such as files on the computer, memory images and registry values.

With the PTS specification, not only can the TPM be used to protect sensitive information, it can also be used to produce irrefutable reports in a standardized format regarding the TPM and the platform as a whole. It can help detect rootkits when used together with boot integrity checking and can identify infected or unauthorized clients.

Trusted Network Connect (TNC)

The TCG has defined the Trusted Network Connect (TNC) architecture and specifications, a set of open standards for Network Access Control. TNC allows IT administrators to define one or more security policies and check each network connected system ("endpoint") for compliance with those policies when the endpoint connects to the network. Endpoints that do not comply with policy can be quarantined and remediated.

TNC can be combined with PTS and TPM to detect endpoints with rootkits, quarantine them, and remediate them. TNC is designed to work with a wide variety of networking equipment so it does not require massive equipment upgrades or replacements. If an endpoint does not have a TPM and PTS, software-only checking can be employed for a lesser level of security.

Copyright ©2004-2006 Trusted Computing Group (www.trustedcomputinggroup.org.) All Rights Reserved